PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04Q 7/38

A1

(11) Internationale Veröffentlichungsnummer: **WO 99/48318**

(43) Internationales Veröffentlichungsdatum: 23. September 1999 (23.09.99)

(21) Internationales Aktenzeichen: PCT/DE99/00362

(22) Internationales Anmeldedatum: 10. Februar 1999 (10.02.99)

(30) Prioritätsdaten:
198 12 215.2 19. März 1998 (19.03.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: FREITAG, Bernhard [DE/DE]; Ginsterweg 11C, D–36251 Bad Hersfeld (DE). BOLZ, Gert [DE/DE]; Neue Strasse 5, D–36154 Hosenfeld (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

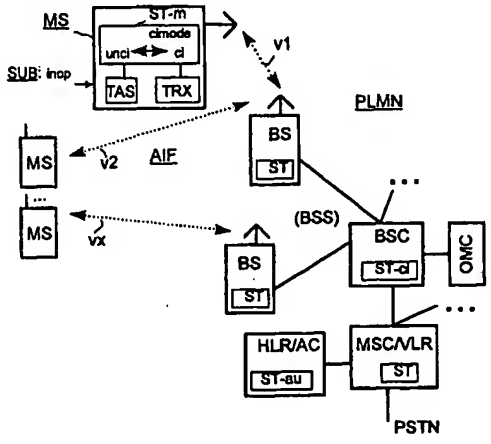
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD, MOBILE STATION AND RADIOCOMMUNICATION SYSTEM FOR CONTROLLING SAFETY RELATED FUNCTIONS IN COMMUNICATION HANDLING

(54) Bezeichnung: VERFAHREN, MOBILSTATION UND FUNK-KOMMUNIKATIONSSYSTEM ZUR STEUERUNG VON SICHERHEITSBEZOGENEN FUNKTIONEN BEI DER VERBINDUNGSBEHANDLUNG

(57) Abstract

On the basis of a well-known method or radiocommunication system for controlling safety related functions in communication handling with subscriber authenticating and non disclosure of information, the mobile station(MS) receives and evaluates a coding request with an answer code (cimode) for determining whether the communication network wishes to establish connections on the radio interface (AIF) with coded or non coded information. Said mobile station (MS) can be switched by the subscriber to an operation mode in which the connection (i.e. v1) is disrupted, when the received characteristic (cimode) authorises communications comprising non coded information. If the radio subscriber wishes that non coded communications are not listened to, it is possible if necessary to guarantee an information subscriber–controlled transmission which prevents people from listening in.



(57) Zusammenfassung

Ausgehend von dem bekannten Verfahren bzw. Funk–Kommunikationssystem zur Steuerung der sicherheitsbezogenen Funktionen bei der Verbindungsbehandlung mit Teilnehmerauthentifikation und Geheimhaltung der Informationen wird eine Verschlüsselungsanforderung mit einer Kennung (cimode), ob das Kommunikationsnetz Verbindungen auf der Funkschnittstelle (AIF) mit verschlüsselten Informationen oder mit unverschlüsselten Informationen wünscht, von der Mobilstation (MS) empfangen und ausgewertet. Dabei ist die Mobilstation (MS) teilnehmergesteuert in einen Betriebsmodus umschaltbar, bei dem die Verbindung (z.B. v1) abgebrochen wird, wenn die empfangene Kennung (cimode) die Verbindungen mit unverschlüsselten Informationen zuläßt. Wird das Abhören unverschlüsselter Verbindungen vom Funkteilnehmer nicht gewünscht, kann teilnehmergesteuert eine abhörsichere Übertragung der Informationen im Bedarfsfall gewährleistet werden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Verfahren, Mobilstation und Funk-Kommunikationssystem zur Steuerung von sicherheitsbezogenen Funktionen bei der Verbindungsbehandlung

Die Erfindung betrifft ein Verfahren, eine Mobilstation und ein Funk-Kommunikationssystem zur Steuerung von sicherheitsbezogenen Funktionen bei der Verbindungsbehandlung gemäß dem Oberbegriff des Patentanspruchs 1 bzw. 6 bzw. 7.

Funk-Kommunikationssysteme, wie beispielsweise das Mobilfunksystem nach dem GSM-Standard (Global System for Mobile Communication), nutzen zur Informationsübertragung eine Funkschnittstelle, auf der Verbindungen zwischen Mobilstationen und Netzeinrichtungen eines Kommunikationsnetzes aufgebaut, abgebaut und aufrechterhalten werden können. Bei der Verbindungsbehandlung werden mobilfunkspezifische Funktionen ausgeführt, zu denen sicherheitsbezogene Funktionen, wie die Teilnehmerauthentifikation und die Geheimhaltungsfunktion, gehören. Durch die üblicherweise mit einem Verbindungsaufbau zwischen Mobilstation und Kommunikationsnetz gestartete Teilnehmerauthentifikation wird die Zugangsberechtigung eines Funkteilnehmers zum Kommunikationsnetz überprüft. Die Geheimhaltungsfunktion basiert auf der Verschlüsselung der über die Funkschnittstelle zu übertragenden Informationen - insbesondere der Nutzinformationen. Eine Verschlüsselungsprozedur wird netzseitig initiiert, indem eine Verschlüsselungsanforderung an die Mobilstation gesendet und mobilstationsseitig mit dem Übermitteln von bereits verschlüsselter Informationen beantwortet wird. Die sicherheitsbezogenen Funktionen sind für ein Funk-Kommunikationssystem nach dem GSM-Standard beispielsweise in „Netzübersicht GSM", Siemens AG, 1995, Kapitel 3.4.2, Seiten 114 ff beschrieben.

Die obige Vorgehensweise basiert auf dem Prinzip, daß die Mobilstation dem Kommunikationsnetz vertraut, d.h. von ihr die

sicherheitsbezogenen Funktionen nicht beeinflußbar sind. Für die bei einer Mobilstation ankommenden oder von ihr abgehenden Verbindungen bedeutet dies, daß - beispielsweise durch besondere Eingriffe auf der Funkschnittstelle, siehe die ältere Patentanmeldung P 19749388.2 - ein gezieltes Abhören (interception) möglich ist, ohne daß die Mobilstation dies verhindern kann. Bei der Lösung gemäß der älteren Patentanmeldung wird nämlich die Mobilstation gezwungen, eine unverschlüsselte Verbindung aufzubauen.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren, ein Funk-Kommunikationssystem und eine Mobilstation der eingangs genannten Art anzugeben, durch das bzw. die das Abhören der Verbindungen auf der Funkschnittstelle sicher vermieden werden kann.

Diese Aufgabe wird gemäß der Erfindung durch das Verfahren mit den Merkmalen des Patentanspruchs 1, das Funk-Kommunikationssystem mit den Merkmalen des Patentanspruchs 6 und durch die Mobilstation mit den Merkmalen des Patentanspruchs 7 gelöst. Vorteilhafte Weiterbildungen der Erfindung sind den Unteransprüchen zu entnehmen.

Ausgehend von dem bekannten Verfahren bzw. Funk-Kommunikationssystem zur Steuerung der sicherheitsbezogenen Funktionen bei der Verbindungsbehandlung mit Teilnehmerauthentifikation und Geheimhaltung der Informationen wird die Verschlüsselungsanforderung mit einer Kennung, ob das Kommunikationsnetz Verbindungen auf der Funkschnittstelle mit verschlüsselten Informationen oder mit unverschlüsselten Informationen wünscht, von der Mobilstation empfangen und ausgewertet. Dabei ist die Mobilstation teilnehmergesteuert in einen Betriebsmodus umschaltbar, bei dem die Verbindung abgebrochen wird, wenn die empfangene Kennung die Verbindungen mit unverschlüsselten Informationen zuläßt.

Die Mobilstation gemäß dem Gegenstand der Erfindung umfaßt eine Steuereinheit zum Auswerten einer vom Kommunikationsnetz übersandten Kennung, die angibt, ob das Kommunikationsnetz Verbindungen auf der Funkschnittstelle mit verschlüsselten Informationen oder mit unverschlüsselten Informationen wünscht. Darüber hinaus ist die Mobilstation teilnehmergesteuert in einen Betriebsmodus umschaltbar, bei dem die Steuereinheit einen Abbruch der Verbindung veranlaßt, wenn die empfangene Kennung die Verbindungen Durch die Erfindung ist sichergestellt, daß die Verbindungen auf der Funkschnittstelle nur mehr verschlüsselte Informationen enthalten, ansonsten droht der mobilstationsseitige Abbruch der Verbindung. Die Mobilstation hat folglich die Möglichkeit, teilnehmergesteuert das Abhören von Verbindungen mit unverschlüsselten Informationen zu unterbinden bzw. zu vermeiden, und braucht sich daher nicht mehr auf das Kommunikationsnetz zu verlassen, wenn dieses unverschlüsselte Informationsübertragung erlaubt und entsprechende Verbindungen initiiert.

Gemäß einer günstigen Weiterbildung der Erfindung ist vorgesehen, daß von der Mobilstation eine Nachricht zum Auslösen der Verbindung über die Funkschnittstelle zum Kommunikationsnetz gesendet wird. Durch das Senden einer Auslösenachricht wird das Kommunikationsnetz direkt und unmittelbar über den Abbruch der Verbindung durch die Mobilstation informiert.

Gemäß einer alternativen Weiterbildung der Erfindung ist vorgesehen, daß von der Mobilstation die Sende/Empfangseinheit zum Senden und Empfangen von Funksignalen vorübergehend abgeschaltet wird, um dem Kommunikationsnetz den Abbruch der Verbindung zu signalisieren.

Eine besonders einfache, aber sehr wirkungsvolle und bedienerfreundliche Möglichkeit zur teilnehmergesteuerten Umschaltbarkeit der Mobilstation in den Betriebsmodus besteht darin, eine gesonderte Stationstaste an der Mobilstation vorzusehen.

Eine dazu alternative oder zusätzliche Weiterbildung der Erfindung sieht vor, durch Eingabeoperationen - vorzugsweise menuegesteuert - die Mobilstation teilnehmergesteuert in den Betriebsmodus zu schalten.

Im folgenden wird die Erfindung anhand eines Ausführungsbeispiels bezugnehmend auf zeichnerische Darstellungen näher erläutert.

Dabei zeigen

FIG 1 das Blockschaltbild eines Funk-Kommunikationssystems zur Steuerung sicherheitsbezogener Funktionen gemäß der Erfindung, und

FIG 2 den Nachrichtenfluß bei der Steuerung der sicherheitsbezogener Funktionen zwischen einer Mobilstation und Netzeinrichtungen eines Kommunikationsnetzes.

Das in FIG 1 dargestellte Funk-Kommunikationssystem entspricht in seiner Struktur einem bekannten GSM-System mit einem TDMA-Vielfachzugriffsverfahren (Time Division Multiple Access) auf einer Funkschnittstelle AIF zur Verbindung von Mobilstationen MS mit Netzeinrichtungen eines Kommunikationsnetzes PLMN. Die Erfindung ist jedoch auch auf andere Funk-Kommunikationssysteme anwendbar, die andere Vielfachzugriffsverfahren - beispielsweise mit einer CDMA-Komponente - nutzen oder einen anderen Netzaufbau aufweisen. Auf der Funkschnittstelle AIF des Funk-Kommunikationssystems laufen mehrere Verbindungen v1, v2...vx zwischen beweglichen Mobilstationen MS und ortsfesten Basisstationen BS des Kommunikationsnetzes PLMN. Eine solche Basisstation BS ist eine Funkstation, die zur Abdeckung eines Funkbereichs - z.B. einer Funkzelle - angeordnet ist, um über die Funkschnittstelle AIF die Verbindungen von/zu den Mobilstationen MS, die sich in ihrem Funk-

bereich aufhalten, aufbauen, abbauen und aufrechthalten zu können. Im vorliegenden Beispiel sei angenommen, daß die Verbindungen v1 und v2 von einer Basisstation BS sowie die Verbindung vx von einer anderen Basisstation BS betreut werden. Bei den Verbindungen kann es sich sowohl um abgehende als auch um ankommende Verbindungen handeln. Jede Basisstation BS ist mit einer Basisstationssteuerung BSC verbunden, deren Anzahl je nach Funkabdeckung des Kommunikationsnetzes variieren kann. Basisstationen BS und Basisstationssteuerungen BSC bilden das für die funktechnischen Funktionen zuständige Basisstationssystem BSS.

Das Kommunikationsnetz PLMN weist darüber hinaus auch Vermittlungseinrichtungen, die Mobilvermittlungsstellen MSC/VLR, auf, die untereinander vernetzt sind bzw. den Zugang zu einem anderen Kommunikationsnetz, z.B. einem Festnetz PSTN, herstellen. Dabei ist der Mobilvermittlungsstelle MSC/VLR eine dezentrale Teilnehmerdatenbasis, das Besucherregister VLR, zur Speicherung von Teilnehmerdaten der in ihrem Zuständigkeitsbereich befindlichen Funkteilnehmer zugeordnet. Die Mobilvermittlungsstelle MSC/VLR ist an die Basisstationssteuerung BSC angeschaltet. Im Kommunikationsnetz PLMN ist weiterhin zumindest eine zentrale Teilnehmerdatenbasis, das Heimatregister HLR, zur Speicherung der Teilnehmerdaten aller im Kommunikationsnetz registrierten Funkteilnehmer vorgesehen. Mit dem Heimatregister in Verbindung steht ein Authentifikationszentrum AC. Ein Operations- und Wartungszentrum OMC realisiert Kontroll- und Wartungsfunktionen im FunkKommunikationssystem bzw. für Teile davon.

Die sicherheitsbezogenen Funktionen bei der Verbindungsbehandlung umfassen die Teilnehmerauthentifikation unter Einbeziehung des Authentifikationszentrums AC sowie die Geheimhaltung der Informationen bei der Übertragung über die Funkschnittstelle AIF unter Einbeziehung des Basisstationssystems BSS. Bekanntlich dient die Teilnehmerauthentifikation zur Überprüfung der Zugangsberechtigung des Funkteilnehmers zum

Kommunikationsnetz PLMN, während die Verschlüsselung bewirkt, daß auf den Übertragungskanälen ausgetauschte Informationen, insbesondere Nutzinformationen, unbefugten Dritten - beispielsweise durch Abhören der Verbindung - nicht zur Verfügung stehen. Jede Netzeinrichtung verfügt üblicherweise über eine Steuereinheit ST. Dabei übernehmen netzseitig eine Steuereinheit ST-ci des Basisstationssystems BSS - beispielsweise in der Basisstationssteuerung BSC - die Funktionen der Verschlüsselungsprozedur (ciphering) sowie eine Steuereinheit ST-au des Authentifikationszentrums AC die Funktionen der Authentifikationsprozedur.

Auch die Mobilstation MS weist Einrichtungen zur Unterstützung der sicherheitsbezogenen Funktionen auf. So verfügt sie bekanntlich über ein Teilnehmermodul - z.B. SIM-Karte - zur Speicherung eines individuellen Teilnehmerschlüssels sowie von Algorithmen für die Berechnung von Sichheitsparametern. Des weiteren weist sie eine Steuereinheit ST-m, eine Sende/Empfangseinheit TRX zum Senden und Empfangen von Funksignalen über die Funkschnittstelle AIF und Eingabemittel zur Benutzung des Endgeräts umfassen Stationstasten - z.B. zur Eingabe von alphanumerischen Zeichen und Operationen. Durch Betätigung einer gesonderten Stationstaste TAS - d.h. teilnehmergesteuert - ist die Mobilstation MS von der Steuereinheit ST-m gemäß der Erfindung in einen Betriebsmodus umschaltbar, bei dem die Verbindung v1 zur Basisstation BS abgebrochen werden kann. Dies ist dann der Fall, wenn eine vom Basisstationssystem BSS empfangene Kennung cimode, die in einer netzseitigen Verschlüsselungsanforderung mitgesendet wird, anzeigt, daß die Verbindung v1 mit unverschlüsselten Informationen benutzt wird. Dazu wertet die Steuereinheit ST-m die eintreffende Kennung cimode aus, die entweder einen Index ci (ciphered) - gleichbedeutend mit dem netzseitigen Wunsch nach verschlüsselter Informationsübertragung - oder einen Index unci (unciphered) - gleichbedeutend mit dem netzseitigen Wunsch nach unverschlüsselter Informationsübertragung - enthält.

Eine zur Betätigung der gesonderten Stationstaste TAS alternative Lösung zum teilnehmergesteuerten Umschalten in den Betriebsmodus, bei dem nur Verbindungen mit verschlüsselten Informationen zulässig sind, besteht darin, daß der Funkteilnehmer SUB bestimmte Eingabeoperationen inop - vorzugsweise menuegesteuert über beispielsweise Funktionstasten der Mobilstation MS - vornimmt. Zum Abbruch des Aufbaus der Verbindung v1 generiert die Steuereinheit ST-m der Mobilstation MS vorzugsweise eine Auslösenachricht, die zum Basistationssystem BSS gesendet wird, um dem Kommunikationsnetz PLMN das Nichtzustandekommen der Verbindung v1 zu signalisieren. Diese Nachricht kann verschlüsselt - unter Anwendung eines in der Mobilstation vorliegenden Verschlüsselungskodes - oder unverschlüsselt erfolgen. Alternativ zum Senden einer eigenen Nachricht kann von der Steuereinheit ST-m der Mobilstation MS auch die Sende/Empfangseinheit TRX für den Abbruch der Verbindung v1 vorübergehend abgeschaltet werden.

Durch die Erfindung ist sichergestellt, daß die Verbindungen v1, v2, vx... auf der Funkschnittstelle AIF nur mehr verschlüsselte Informationen enthalten, ansonsten droht der mobilstationsseitige Abbruch der jeweiligen Verbindung. Die Mobilstation MS hat folglich die Möglichkeit, teilnehmergesteuert das Abhören von Verbindungen mit unverschlüsselten Informationen zu unterbinden bzw. zu vermeiden, und braucht sich daher nicht mehr auf das Kommunikationsnetz zu verlassen, wenn dieses unverschlüsselte Informationsübertragung erlaubt und entsprechende Verbindungen initiiert, die von Dritten abhörbar sind. Befindet sich die Mobilstation in dem Betriebsmodus unci und erlaubt der Funkteilnehmer auch die unverschlüsselte Informationsübertragung über vom Kommunikationsnetz PLMN zur Verfügung gestellten Verbindungen, können auch entsprechende unverschlüsselte Verbindungen auf der Funkschnittstelle AIF aufgebaut werden.

FIG 2 zeigt in schematischer Darstellung den Nachrichtenfluss

zur Steuerung der sicherheitsbezogenen Funktionen im Funk-Kommunikationssystem gemäß FIG 1. Die am Nachrichtenfluß beteiligten Einrichtungen sind die Mobilstation MS mit der Steuereinheit ST-m, das Basisstationssystem BSS mit der Steuereinheit ST-ci, die Mobilvermittlungsstelle MSC/VLR mit der Steuereinheit ST und das Heimatregister HLR bzw. Authentifikationszentrum AC mit der Steuereinheit ST-au. Die Steuereinheit ST-m erzeugt eine Verbindungsaufbaunachricht vreq - beispielsweise zur Aufenthaltsregistrierung, zum Austausch von Kurznachrichten, zum „Location Update" bei Wechsel des Versorgungsbereichs durch ein anderes Besucherregister VLR usw. - und sendet sie auf einem Kontrollkanal - beispielsweise dem BCCH-Kontrollkanal (Broadcast Control Channel) - zur Mobilvermittlungsstelle MSC/ VLR. Die Anforderung vreq enthält eine Teilnehmeridentität imsi, eine Ortsinformation lai und eine Gerätekennung imei. Das Besucherregister VLR leitet daraufhin die Authentifikation durch Senden einer Authentifikationsanfrage aureq an das Heimatregister HLR bzw. Authentifikationszentrum AC ein. Falls dem Besucherregister VLR die Teilnehmerdaten noch nicht bekannt sind, fordert sie mit diesen Daten vom Heimatregister HLR zusätzlich die Sicherheitsparameter (triplets) an. Das Heimatregister HLR holt sich die geforderten Sicherheitsparameter vom Authentifikationszentrum AC ab und sendet sie zusammen mit den Teilnehmerdaten in einer Authentifikationsantwort aures in der Gegenrichtung zurück. Die Sicherheitsparameter umfassen eine Zufallszahl RAND, einen individuellen Teilnehmerschlüssel Ki, eine Authentifikationsantwort SRES (Signed Response) und einen Verschlüsselungskode Kc.

Die Mobilvermittlungsstelle MSC/VLR sendet die Zufallszahl RAND über die netzseitig für die Mobilstation MS zuständige Basisstation des Basisstationssystems BSS zum Endgerät. Die Mobilstation MS bzw. deren Steuereinheit ST-m berechnet ihrerseits die Authentifikationsantwort SRES anhand eines vorgebbaren Algorithmus aus der übermittelten Zufallszahl RAND und des im Teilnehmermodul gespeicherten Teilnehmerschlüs-

sels. Darüber hinaus bestimmt sie den Verschlüsselungskode Kc anhand eines anderen Algorithmus und den vorstehend genannten Parametern. Anschließend sendet sie die berechnete Authentifikationsantwort SRES für einen Vergleich mit der netzseitig gespeicherten Authentifikationsantwort SRES zum Besucherregister VLR. Ergibt der Vergleich eine Identität der Antworten SRES, ist die Teilnehmerauthentifikation erfolgreich, andererseits kann ein Eintrag in eine Sicherheitsdatei des Besucherregisters VLR erfolgen. Ausgehend von der erfolgreich durchgeführten Authentifikation sendet das Besucherregister VLR den berechneten Verschlüsselungskode Kc zum Basisstationssystem BSS, das für die netzseitige Verschlüsselung der Informationen auf der Funkschnittstelle verantwortlich ist.

Das Basisstationssystem BSS generiert eine Verschlüsselungsanforderung cireq zum Verschlüsseln der auf der Funkschnittstelle zu übertragenden Informationen in Richtung Mobilstation MS und sendet darin die Kennung cimode, ob das Kommunikationsnetz PLMN Verbindungen auf der Funkschnittstelle mit verschlüsselten Informationen oder mit unverschlüsselten Informationen wünscht, mit. Vorzugsweise wird die Kennung cimode von der in der Basisstationssteuerung enthaltenen Steuereinheit ST-ci erzeugt und in die Nachricht cireq eingefügt. Von der Steuereinheit ST-m wird die empfangene Kennung cimode ausgewertet. Falls die Mobilstation MS teilnehmergesteuert in den Betriebsmodus mit dem Index ci geschaltet ist und die Auswertung der Kennung cimode nur die Nutzung von Verbindungen mit verschlüsselten Informationen identifiziert, generiert sie eine Verschlüsselungsantwort cires, in der die Informationen bereits verschlüsselt mit dem Kode Kc in der Aufwärtsrichtung zum Kommunikationsnetz bzw. zur Mobilvermittlungsstelle MSC/VLR übertragen werden. Im Anschluß an die Nachricht cires wird der Verbindungsaufbau fortgesetzt und eine Verbindungsaufbauantwort setup von der Mobilvermittlungsstelle MSC/VLR in der Abwärtsrichtung zur Mobilstation MS übertragen.

Andernfalls, wenn folglich die Auswertung der Kennung cimode anhand des Index unci die Nutzung von Verbindungen mit unverschlüsselten Informationen identifiziert, generiert die Steuereinheit ST-m der Mobilstation MS eine Auslösenachricht rel. Die Auslösenachricht rel signalisiert, daß die Verbindung abgebrochen wird, da die empfangene Kennung cimode auch unverschlüsselte Informationsübertragung zuläßt, die Mobilstation MS aber sich in dem Betriebsmodus für lediglich verschlüsselte Verbindungen befindet. Das Abhören unverschlüsselter Verbindungen wird vom Funkteilnehmer nicht gewünscht. Daher hat er die Mobilstation MS in den zugehörigen Betriebsmodus geschaltet, um eine abhörsichere Übertragung im Bedarfsfall teilnehmergesteuert gewährleisten zu können. Die Auslösenachricht rel kann verschlüsselt oder unverschlüsselt über die Funkschnittstelle zum Basisstationssystem BSS gesendet werden.

Patentansprüche

1. Verfahren zur Steuerung von sicherheitsbezogenen Funktionen bei der Verbindungsbehandlung in einem Funk-Kommunikationssystem mit einer Funkschnittstelle (AIF) zur Anbindung von Mobilstationen (MS) an ein Kommunikationsnetz (PLMN), bei dem
- sobald ein Verbindungsaufbau von der Mobilstation (MS) initiiert ist, eine Teilnehmerauthentifikation zur Überprüfung der Zugangsberechtigung eines Funkteilnehmers zum Kommunikationsnetz (PLMN) zwischen der Mobilstation (MS) und dem Kommunikationsnetz (PLMN) durchgeführt wird, und
- eine Verschlüsselungsanforderung (cireq) zur Geheimhaltung der Informationen auf der Funkschnittstelle vom Kommunikationsnetz (PLMN) an die Mobilstation (MS) gesendet wird,
d a d u r c h g e k e n n z e i c h n e t,
daß die Verschlüsselungsanforderung (cireq) mit einer Kennung (cimode), ob das Kommunikationsnetz (PLMN) Verbindungen auf der Funkschnittstelle (AIF) mit verschlüsselten Informationen oder mit unverschlüsselten Informationen wünscht, von der Mobilstation (MS) empfangen und ausgewertet wird, und
daß die Mobilstation (MS) teilnehmergesteuert in einen Betriebsmodus umschaltbar ist, bei dem die Verbindung (z.B. v1) abgebrochen wird, wenn die empfangene Kennung (cimode) die Verbindungen mit unverschlüsselten Informationen zuläßt.

2. Verfahren nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t,
daß von der Mobilstation (MS) eine Nachricht (rel) zum Auslösen der Verbindung (z.B. v1) über die Funkschnittstelle (AIF) zum Kommunikationsnetz (PLMN) gesendet wird.

3. Verfahren nach Anspruch 1,
d a d u r c h g e k e n n z e i c h n e t,
daß von der Mobilstation (MS) die zum Senden und Empfangen von Funksignalen vorgesehene Sende/Empfangseinheit (TRX) für

den Abbruch der Verbindung (z.B. v1) vorübergehend abgeschaltet wird.

4. Verfahren nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
daß durch Betätigung einer gesonderten Stationstaste (TAS) die Mobilstation (MS) teilnehmergesteuert in den Betriebsmodus geschaltet wird.

5. Verfahren nach einem der vorhergehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t,
daß durch Eingabeoperationen (inop) die Mobilstation (MS) teilnehmergesteuert in den Betriebsmodus geschaltet wird.

6. Funk-Kommunikationssystem zur Steuerung von sicherheitsbezogenen Funktionen bei der Verbindungsbehandlung, mit
- einer Funkschnittstelle (AIF) zur Anbindung von Mobilstationen (MS) an ein Kommunikationsnetz (PLMN),
- Netzeinrichtungen (BSS, MSC/VLR, HLR/AC) zur Durchführung einer Teilnehmerauthentifikation für eine Überprüfung der Zugangsberechtigung eines Funkteilnehmers zum Kommunikationsnetz (PLMN), sobald ein Verbindungsaufbau von der Mobilstation (MS) initiiert ist, und mit
- Netzeinrichtungen (BSS) zum Senden einer Verschlüsselungsanforderung (cireq) für eine Geheimhaltung der Informationen auf der Funkschnittstelle an die Mobilstation (MS),
d a d u r c h g e k e n n z e i c h n e t,
daß die Netzeinrichtungen (BSS) eine Steuereinheit (ST-ci) zum Einfügen einer Kennung (cimode), ob das Kommunikationsnetz (PLMN) Verbindungen auf der Funkschnittstelle mit verschlüsselten Informationen oder mit unverschlüsselten Informationen wünscht, in die Verschlüsselungsanforderung (cireq) aufweisen,
daß die Mobilstation (MS) eine Steuereinheit (ST-m) zum Auswerten der empfangenen Kennung (cimode) aufweist, und
daß die Mobilstation (MS) teilnehmergesteuert in einen Betriebsmodus umschaltbar ist, bei dem die Steuereinheit (ST-m)

einen Abbruch der Verbindung (z.B. v1) veranlaßt, wenn die empfangene Kennung (cimode) die Verbindungen mit unverschlüsselten Informationen zuläßt.

7. Mobilstation zur Steuerung von sicherheitsbezogenen Funktionen bei der Verbindungsbehandlung in einem Funk-Kommunikationssystem mit einer Funkschnittstelle (AIF) zur Anbindung der Mobilstation (MS) an ein Kommunikationsnetz (PLMN), das Netzeinrichtungen (BSS, MSC/VLR, HLR/AC) zur Durchführung einer Teilnehmerauthentifikation für eine Überprüfung der Zugangsberechtigung eines Funkteilnehmers zum Kommunikationsnetz (PLMN), sobald ein Verbindungsaufbau von der Mobilstation (MS) initiiert ist, und Netzinrichtungen (BSS) zum Senden einer Verschlüsselungsanforderung (cireq) für eine Geheimhaltung der Informationen auf der Funkschnittstelle an die Mobilstation (MS) aufweist,
d a d u r c h g e k e n n z e i c h n e t,
daß die Mobilstation (MS) eine Steuereinheit (ST-m) zum Auswerten einer vom Kommunikationsnetz (PLMN) übersandten Kennung (cimode) aufweist, die angibt, ob das Kommunikationsnetz (PLMN) Verbindungen auf der Funkschnittstelle (AIF) mit verschlüsselten Informationen oder mit unverschlüsselten Informationen wünscht, und
daß die Mobilstation (MS) teilnehmergesteuert in einen Betriebsmodus umschaltbar ist, bei dem die Steuereinheit (ST-m) einen Abbruch der Verbindung (z.B. v1) veranlaßt, wenn die empfangene Kennung (cimode) die Verbindungen mit unverschlüsselten Informationen zuläßt.

8. Mobilstation nach Anspruch 7,
d a d u r c h g e k e n n z e i c h n e t,
daß die Steuereinheit (ST-m) der Mobilstation (MS) eine Nachricht (rel) zum Auslösen der Verbindung erzeugt und über die Funkschnittstelle (AIF) zum Kommunikationsnetz (PLMN) sendet.

9. Mobilstation nach Anspruch 7 oder 8,
d a d ü r c h g e k e n n z e i c h n e t,

daß eine gesonderte Stationstaste (TAS) vorgesehen ist, durch deren Betätigung teilnehmergesteuert die Mobilstation (MS) in den Betriebsmodus umschaltbar ist.

10. Mobilstation nach Anspruch 7, 8 oder 9,
d a d u r c h g e k e n n z e i c h n e t,
daß Eingabeoperationen (inop) vorgesehen sind, durch die die Mobilstation (MS) teilnehmergesteuert in den Betriebsmodus umschaltbar ist.

1/2

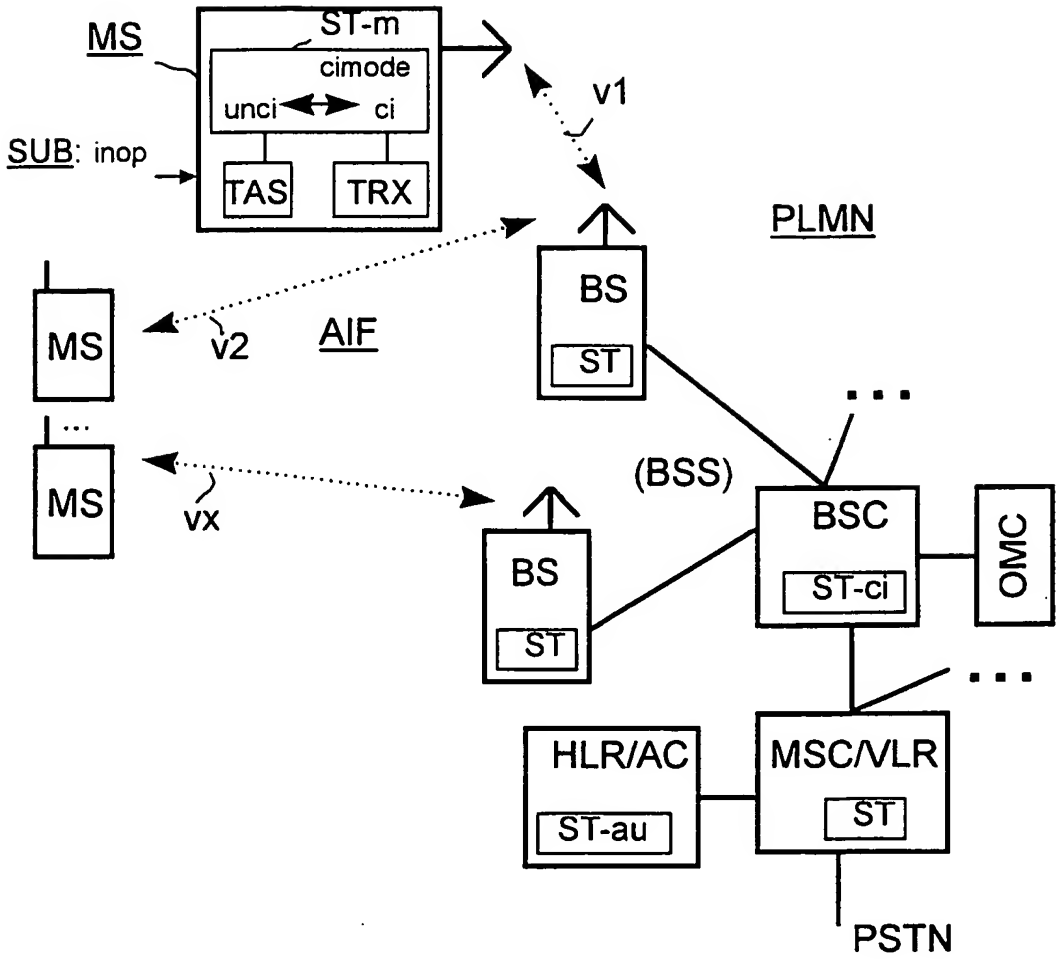

MS
ST-m
cimode
unci
ci
SUB: inop
TAS
TRX
v1
PLMN
BS
ST
MS
v2
AIF
MS
vx
(BSS)
BSC
ST-ci
OMC
BS
ST
HLR/AC
ST-au
MSC/VLR
ST
PSTN

FIG 1

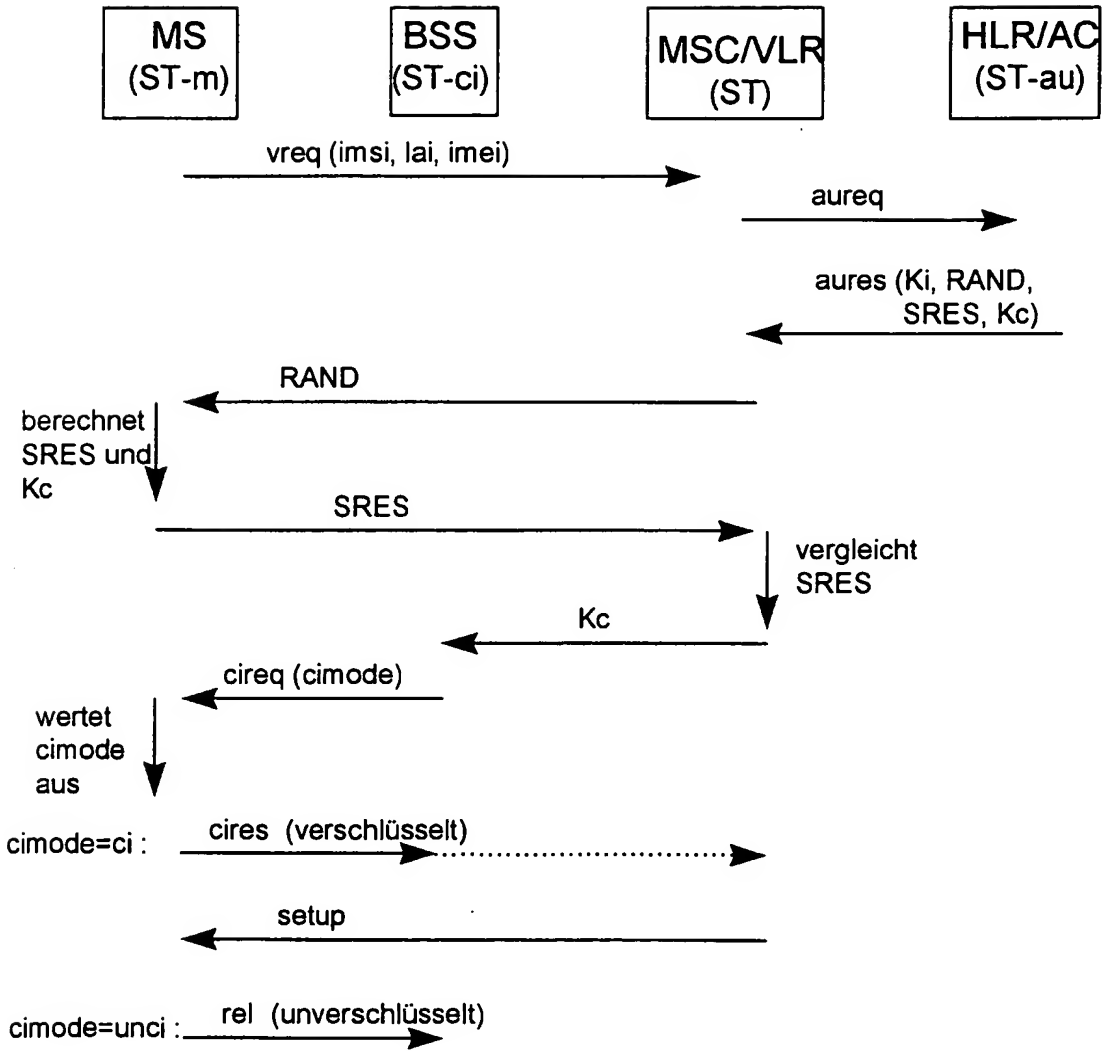

MS
(ST-m)
BSS
(ST-ci)
MSC/VLR
(ST)
HLR/AC
(ST-au)
vreq (imsi, lai, imei)
aureq
aures (Ki, RAND,
SRES, Kc)
RAND
berechnet
SRES und
Kc
SRES
vergleicht
SRES
Kc
cireq (cimode)
wertet
cimode
aus
cimode=ci :
cires (verschlüsselt)
setup
cimode=unci :
rel (unverschlüsselt)

FIG 2

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/DE 99/00362

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04M H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 779 760 A (NOKIA MOBILE PHONES LTD) 18 June 1997 (1997-06-18) column 4, line 3 - column 7, line 14 ---	1,6,7
A	EP 0 827 356 A (NOKIA MOBILE PHONES LTD) 4 March 1998 (1998-03-04) column 3, line 30 - column 6, line 39 -----	1,6,7

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search
8 July 1999

Date of mailing of the international search report
14/07/1999

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer
Kampouris, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ional Application No
PCT/DE 99/00362

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0779760 A	18-06-1997	FI 956036 A	16-06-1997
EP 0827356 A	04-03-1998	FI 963428 A	03-03-1998

INTERNATIONALER RECHERCHENBERICHT

Inte. onales Aktenzeichen
PCT/DE 99/00362

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04Q7/38

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04M H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 779 760 A (NOKIA MOBILE PHONES LTD) 18. Juni 1997 (1997-06-18) Spalte 4, Zeile 3 - Spalte 7, Zeile 14 ---	1,6,7
A	EP 0 827 356 A (NOKIA MOBILE PHONES LTD) 4. März 1998 (1998-03-04) Spalte 3, Zeile 30 - Spalte 6, Zeile 39 -----	1,6,7

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
8. Juli 1999	14/07/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Kampouris, A

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlich. , .n. die zur selben Patentfamilie gehören

Inter .nales Aktenzeichen
PCT/DE 99/00362

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0779760 A	18-06-1997	FI 956036 A	16-06-1997
EP 0827356 A	04-03-1998	FI 963428 A	03-03-1998